Zaw-Sing Su
SRI
May 1981

A SPECIFICATION OF THE INTERNET PROTOCOL (IP) TIMESTAMP OPTION

I. INTRODUCTION

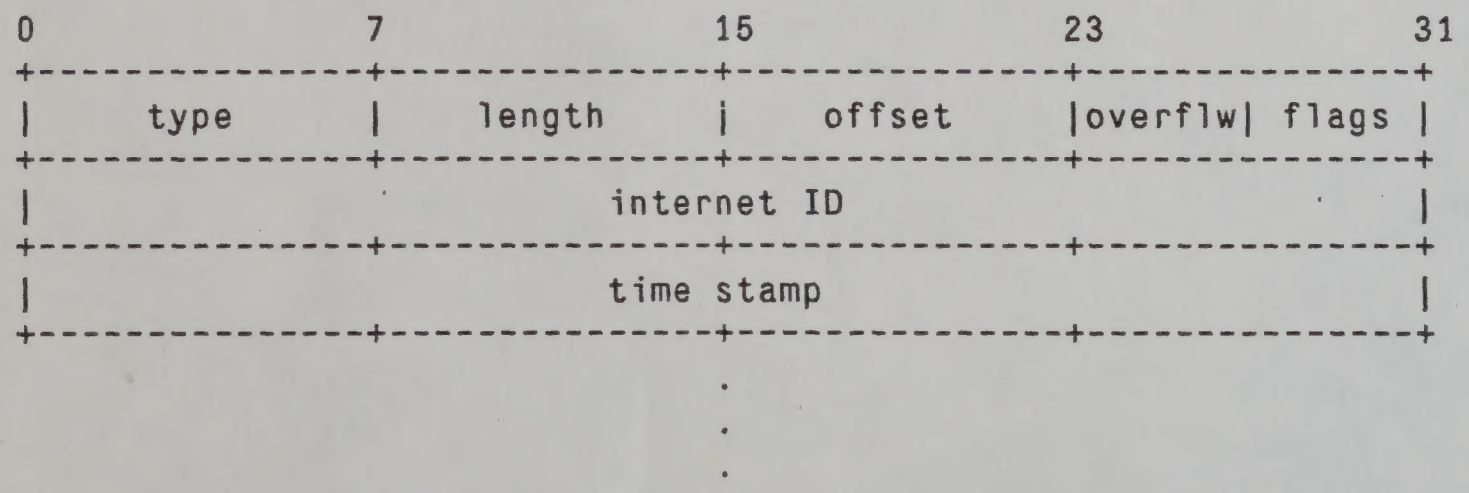
Packet switching is store-and-forward by nature. Network delay is a therefore a critical performance measure for packet-switching communications. A catenet is a system of packet-switched communication networks interconnected via gateways [Cerf 78]. The catenet "link" delays are thus variable. Their measurement, the measurement of delays across member networks of a catenet, becomes important for catenet investigations.

An effective way to measure catenet delays is by means of packet header timestamping. Header timestamping allows monitoring of catenet delays for user traffic, such as the case of Ft. Bragg users accessing ISID across the catenet. Packet header timestamping is also compatible with the use of test packets for catenet delay measurement. Another advantage of header timestamping is that since it is an IP option, the gateway imposes little difference in the treatment of such a packet. In this note, a specification of the timestamp option format for IP is presented.

Measurement of one-way delay, either end-to-end or across an individual network, requires that device clocks be synchronized, using such facilities as WWVB clocks [Mills 81]. This specification assumes this capability in the gateways and involved network hosts.

II. FORMAT SPECIFICATION

As an IP option, the contents of the first two octets are dictated by the IP header format to be option type and option length in octets [Postel 80]. The next two octets are used to control this option.



option type = 68 decimal (i.e., option class = 2 and option number = 4);

option length = the number of octets with a maximum of 40 (limited by IHL = 15);

offset = the number of octets from the beginning of this option to the end of timestamps (i.e., the beginning of space for next timestamp). It is set to one, an odd number, when no more space remains in the header for timestamps;

overflow = the number of IP modules that cannot register timestamps due to lack of space;

flag = 0 -- time stamps only
1 -- each timestamp is preceded with internet ID of the registering entity
3 -- the internet ID fields are prespecified. An IP module only registers its timestamp if it matches its own ID with the next specified internet ID;

internet ID = ID for the timestamping device;

timestamp = a right-justified, 32-bit timestamp in milliseconds modulo 24 hours from midnight UT.

The timestamp option is not copied upon fragmentation. It is carried in the first fragment.

REFERENCES

[Cerf 78] Cerf, V., "The Catenet Model for Internetworking," Defense Advanced Research Projects Agency, Information Processing Techniques Office, IEN 48, July 1978.

[Mills 81] Mills, D.L., "DCNET Internet Clock Service," RFC 778, COMSAT Laboratories, April 1981.

[Postel 80] Postel, J. (ed.), "DoD Standard Transport Internet Protocol," Defense Advanced Reseach Projects Agency, Information Processing Techniques Office, RFC 760, IEN 128, January 1980.